CA IdentityMinder™

Notes de parution

r12.6.1



Produits CA Technologies référencés

Ce document fait référence aux produits CA Technologies suivants :

- CA IdentityMinder ™
- CA SiteMinder®
- CA Directory
- CA User Activity Reporting (CA UAR)
- CA CloudMinder™ Identity Management
- GovernanceMinder (anciennement CA Role & Compliance Manager)

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Table des matières

Chapitre 1: Nouvelles fonctionnalités 9

Chapitre 2: Remarques relatives à l'installation 25

Chapitre 1: Nouvelles fonctionnalités

Ce chapitre traite des sujets suivants :

12.6.1

Nouvelles certifications

Les nouvelles plates-formes suivantes sont certifiées avec CA IdentityMinder r12.6.1 :

Terminaux

- Microsoft SQL 2012 comme terminal statique et dynamique
- CA Directory r12 SP10 CR2 comme terminal JNDI
- CA Embedded Entitlements Manager (EEM) : pris en charge par le gestionnaire de provisionnement

Référentiel d'utilisateurs CA IdentityMinder

- CA Directory r12 SP10 CR2

Référentiel d'utilisateurs et référentiel d'exécution CA IdentityMinder

- Microsoft SQL Server 2012

Prise en charge supplémentaire

- Mozilla Firefox 14.x
- Serveur de rapports BusinessObjects XI 3.1 SP5 (CA Business Intelligence 3.3)

  Cette version correspond à la version prise en charge par SiteMinder.
- Prise en charge du serveur de rapports dans une configuration de haute disponibilité
- Prise en charge de CA IdentityMinder avec CA GovernanceMinder (CA RCM) r12.6
- Prise en charge de CA IdentityMinder avec CA SiteMinder r12.0 SP3 CR11

Référentiel d'utilisateurs de domaine JNDI compatible SSL

La vérification de certificat d'homologue est désormais appliquée. Cette fonctionnalité requiert l'ajout du certificat de serveur SSL du référentiel d'utilisateurs dans le référentiel de clés approuvé par défaut du JRE CA IdentityMinder. Le référentiel de clés est le fichier cacerts ou jssecacerts sous :

JAVA_HOME\jre\lib\

Prise en charge des applications mobiles

L'application mobile CA IdentityMinder permet d'exploiter l'infrastructure CA IdentityMinder existante pour permettre aux utilisateurs d'effectuer les tâches suivantes sur une unité mobile, tel qu'un iPhone ou un iPad :

- Réinitialiser un mot de passe oublié

  Remarque : Lorsque vous permettez aux utilisateurs mobiles de réinitialiser un mot de passe oublié à partir de leur unité, CA IdentityMinder utilise la sécurité de l'unité au lieu de questions de sécurité. Considérez renforcer la sécurité de l'unité, avec un code secret par exemple, avant d'activer la fonctionnalité de réinitialisation de mot de passe.

- Modifier un mot de passe
- Répondre aux demandes d'approbation
- Afficher les détails du responsable

  Cette fonctionnalité permet aux utilisateurs qui approuvent des demandes de flux de travaux d'afficher les informations sur le responsable d'un utilisateur.

Remarque : Pour plus d'informations sur l'application mobile, consultez le *Manuel d'administration*.

12.6

Nouveau nom et apparence

Dans cette version, CA Identity Manager a été renommé CA IdentityMinder. Tous les produits de sécurité CA ont été renommés pour refléter le nom de la famille de produits Minder. Cette modification facilite l'identification des produits de sécurité CA et renforce la cohésion des solutions de sécurité CA.

En outre, la console d'utilisateur par défaut a été mise à jour pour refléter le nouveau style et couleurs de CA.

Le serveur de connecteurs Java (JCS) a été renommé serveur de connecteurs CA IAM (CA IAM CS).

Expérience utilisateur simplifiée

Cette version inclut les améliorations de l'expérience utilisateur suivantes :

- Fenêtres de tâche d'auto-administration mises à jour

  Les fenêtres suivantes ont été mises à jour pour améliorer la facilité d'utilisation :

  - Apparence du portail pour la fenêtre de connexion
  - Auto-enregistrement/création d'identité
  - Modifier mon mot de passe
  - Réinitialisation du mot de passe oublié
  - ID de l'utilisateur oublié

- Certaines tâches d'administration utilisent des contrôles Web 2.0.

Améliorations du provisionnement

CA IdentityMinder 12.6 inclut les nouvelles fonctionnalités et les modifications suivantes pour améliorer le provisionnement.

Serveur de provisionnement sur Linux

Outre Solaris, vous pouvez dorénavant installer le serveur de provisionnement sur Red Hat Linux.

Fonctionnalités du gestionnaire de provisionnement dans la console d'utilisateur

Plusieurs fonctionnalités du gestionnaire de provisionnement sont prises en charge dans la console d'utilisateur :

- Synchronisation d'utilisateurs, de rôles, de comptes de terminal et de modèles de compte

  L'intégration de terminaux et de comptes dans CA IdentityMinder peut entraîner la perte de la synchronisation. Par exemple, les rôles de provisionnement affectés à un utilisateur peuvent différer des comptes réels de cet utilisateur. Les tâches de synchronisation corrigent ce problème.

- Les règles de corrélation contrôlent le mappage des attributs de compte de terminal aux attributs d'utilisateur dans la console d'utilisateur. Par exemple, CA Access Control a un attribut appelé AccountName. Vous pouvez créer une règle pour le mapper vers FullName dans la console d'utilisateur.

Améliorations des connecteurs

CA IdentityMinder 12.6 inclut les nouvelles fonctionnalités et les modifications suivantes pour simplifier la création et le déploiement de nouveaux connecteurs.

Déploiement à chaud : installez un nouveau connecteur sans redémarrer CA IAM CS.

Le serveur de connecteurs CA IAM (CA IAM CS) est le nouveau nom du serveur de connecteurs Java (Java CS ou JCS).

CA IAM CS prend désormais en charge le *déploiement à chaud*. Le déploiement à chaud est le processus d'ajouter, de supprimer ou de mettre à jour un composant sans redémarrer CA IAM CS. Vous pouvez exécuter les tâches suivantes :

- Installer, désinstaller ou mettre à niveau un connecteur *sans* redémarrer CA IAM CS

  Vous pouvez déployer un nouveau connecteur ou un connecteur mis à jour, et l'installer sans redémarrer CA IAM CS ou vous connecter à son hôte. Contactez le support de CA pour obtenir les dernières versions de connecteur.

- Déployer des bibliothèques tierces sans redémarrer CA IAM CS

  Certains connecteurs requièrent des bibliothèques qui ne peuvent pas être incluses avec CA IAM CS. Vous devrez déployer ces bibliothèques au préalable et redémarrer CA IAM CS. Vous pouvez ensuite déployer ces bibliothèques lors de l'exécution du serveur de connecteurs.

  CA IAM CS inclut un ensemble principal de bibliothèques tierces que tous les connecteurs peuvent utiliser. Un connecteur peut également inclure une autre bibliothèque tierce requise.

Remarque : Le déploiement à chaud ne fonctionne pas pour les connecteurs en C++.

Générateur de groupe : nouvel outil pour la création de connecteurs

CA IAM CS requiert que les connecteurs soient fournis dans un groupe Open Services Gateway initiative. La structure OSGi est un système de module et de plate-forme de service pour le langage de programmation Java qui implémente un modèle de composant complet et dynamique. Le kit de développement logiciel pour le serveur de connecteurs inclut l'outil de générateur de groupe, qui vous permet d'encapsuler le connecteur dans un groupe.

Journalisation pour les connecteurs et CA IAM CS

Vous pouvez désormais vous connecter à CA IAM CS pour afficher les messages de journaux récents pour CA IAM CS et ses connecteurs. Vous pouvez toujours utiliser les fichiers journaux pour afficher tous les messages contenus dans le journal.

Certificats pour les connecteurs et CA IAM CS

Vous pouvez désormais vous connecter à CA IAM CS pour afficher et gérer des certificats pour CA IAM CS et ses connecteurs.

Utilisation de Connector Xpress pour mapper des attributs personnalisés et des attributs de capacité personnalisés

Utilisez Connector Xpress pour mapper des attributs personnalisés et des attributs de capacité personnalisés. L'utilisation du fichier XML <jcs-home>/conf/override/lnd/lnd_custom_metatdata.xml pour mapper des attributs n'est plus possible.

Configuration de CA IAM CS en tant que proxy pour le serveur de connecteurs C++

CA IdentityMinder utilise désormais CA IAM CS comme proxy pour le serveur de connecteurs C++. Aucune communication directe ne se produit entre CA IdentityMinder et le serveur de connecteurs C++.

Améliorations des performances

Des améliorations de performances ont été apportées dans les parties suivantes de CA IdentityMinder 12.6.

Améliorations des performances du chargeur en bloc

Dans cette version, les performances du chargeur en bloc ont été améliorées. Les modifications apportées comprennent notamment :

- Un taux de soumission de tâches plus élevé via la tâche de chargeur en bloc parent : un plus grand nombre de tâches s'exécutent simultanément.
- Des optimisations dans la réutilisation de la connexion à la base de données : la mise en cache des définitions d'attributs d'objet géré aboutit à une exécution plus rapide des tâches du début à la fin.
- Des améliorations de certains modules d'extension et écouteurs pour accélérer le traitement des événements générés pendant l'exécution des tâches.

Pour encore améliorer les performances, il est recommandé d'effectuer les modifications suivantes pour la durée des opérations de chargement en bloc :

  - Désactiver toutes les stratégies Policy Xpress, les gestionnaires de tâches métier et les indicateurs de synchronisation superflus au niveau de la tâche.
  - Exécuter la tâche de chargeur en bloc en tant qu'utilisateur dédié avec le moins possible de rôles d'administration et de tâches d'administration dans la portée.

Remarque : Pour plus d'informations sur les améliorations de performances supplémentaires, consultez la section sur le chargeur en bloc du *Manuel d'administration*.

Performances d'exportation de cliché améliorées

Dans cette version, le processus d'exportation des données de cliché pour des rapports a été mis à jour afin d'améliorer les performances et la facilité d'utilisation. A l'aide de l'Assistant de définition de cliché, vous définissez ou personnalisez les règles de chargement des utilisateurs, des terminaux, des rôles d'administration, des rôles de provisionnement, des groupes et des organisations.

Cette fonctionnalité vous permet d'utiliser une tâche de console d'utilisateur pour sélectionner et exporter uniquement les attributs souhaités pour une instance de cliché. Dans les versions précédentes, vous deviez modifier un fichier XML manuellement.

Remarque : Vous pouvez toujours utiliser et personnaliser les fichiers XML par défaut afin de capturer des clichés.

Pour plus d'informations sur la création des définitions de cliché, reportez-vous au *Manuel d'administration*.

Améliorations de Policy Xpress

Les améliorations suivantes ont été apportées à Policy Xpress dans cette version :

- Modules d'extension d'attribut pour les objets gérés

  Les modules d'extension d'attribut d'objet géré suivants ont été ajoutés à Policy Xpress :

  - Attribut d'objet : permet d'extraire la valeur d'un attribut d'objet géré.
  - Possède un attribut d'objet modifié/Attribut d'objet spécifique : identiques aux modules d'extension Possède une valeur d'attribut d'utilisateur modifiée et Attribut d'un utilisateur, mais ils peuvent être utilisés avec tous les types d'objet géré.
  - Définir les valeurs d'objets : permet de modifier l'attribut des objets gérés.

- Fonction Supprimer

  La fonction Supprimer vous permet de supprimer les espaces de début et de fin superflus d'un élément de données ou d'une chaîne.

- Prise en charge de règles d'action supplémentaires

  Dans les versions précédentes, lorsque vous vouliez ajouter entre 60 et 70 règles d'action à une stratégie, Policy Xpress ne les ajoutait pas. Aucune erreur ou exception n'était incluse dans les journaux. Désormais, les stratégies Policy Xpress peuvent prendre en charge jusqu'à 500 règles d'action.

- Wiki de Policy Xpress

  La documentation de Policy Xpress a été mise à jour et se trouve dans un Wiki https://communities.ca.com/web/ca-identity-and-access-mgmt-distributed-global-user-community/wiki/-/wiki/Main/Policy+Xpress?&#p_36 de la communauté internationale d'utilisateurs des produits de sécurité CA.

Console de gestion sécurisée

La console de gestion permet aux administrateurs de créer et de gérer des annuaires et des environnements CA IdentityMinder.

L'installation de CA IdentityMinder inclut une option sélectionnée par défaut, qui permet de sécuriser la console de gestion. Au cours de l'installation, vous créez un compte qui peut accéder à la console de gestion dans un annuaire prédéfini.

Après l'installation, vous pouvez ajouter les administrateurs supplémentaires qui doivent accéder à la console de gestion.

Remarque : Pour plus d'informations, reportez-vous au *Manuel de configuration*.

Demandes d'accès de base

Les utilisateurs de CA IdentityMinder peuvent demander l'accès aux services dont ils ont besoin pour effectuer leurs fonctions.

Un *service* regroupe tous les droits (tâches, rôles, groupes et attributs) dont un utilisateur a besoin pour un rôle professionnel donné. L'utilisateur peut accéder aux services par l'intermédiaire de tâches de demande d'accès, dans la console d'utilisateur de CA IdentityMinder. Les tâches Demande d'accès permettent à un utilisateur ou à un administrateur de demander, d'affecter, de retirer et de renouveler un service.

Les services permettent aux administrateurs de combiner des droits d'utilisateur dans un package unique et de les gérer comme un ensemble. Par exemple, tous les nouveaux employés des ventes ont besoin d'accéder à un ensemble défini de tâches et de comptes sur des systèmes d'extrémité spécifiques. Ils ont également besoin d'informations spécifiques qui doivent être ajoutées à leurs profils de compte d'utilisateur. Un administrateur crée un service nommé Administration des ventes, contenant toutes les tâches, les rôles, les groupes et les informations d'attribut de profil requis pour un nouvel employé des ventes. Lorsqu'un administrateur affecte le service Administration des ventes à un utilisateur, cet utilisateur reçoit l'intégralité de l'ensemble des rôles, tâches, groupes et attributs de compte définis par le service.

Les utilisateurs peuvent également accéder aux services en effectuant eux-mêmes une demande d'accès. Dans la console d'utilisateur, chaque utilisateur dispose d'une liste des services disponibles qu'il peut demander. Cette liste contient les services définis sur Auto-abonnement par un administrateur avec des droits appropriés, généralement pendant la création du service. A partir de la liste des services disponibles, les utilisateurs peuvent demander l'accès aux services dont ils ont besoin. Lorsqu'un utilisateur demande l'accès à un service, la demande est exécutée automatiquement et les droits associés sont affectés à l'utilisateur immédiatement. Un administrateur disposant des droits appropriés peut également configurer l'exécution des services de sorte à requérir l'approbation de flux de travaux ou à générer des notifications par courriel.

Remarque : La version initiale prend en charge les fonctionnalités de demande d'accès de base. La fonctionnalité de demande d'accès permet aux utilisateurs finals de demander des droits gérés et non gérés par CA IdentityMinder, de définir des flux d'approbation et d'utiliser des flux d'exécution.

Cette version ne prend pas en charge les fonctionnalités de demande d'accès avancées suivantes :

- Définition en bloc d'objets de services de demande d'accès
- Intégration à GovernanceMinder (antérieurement appelé CA Role and Compliance Manager)
- Filtres et recherches détaillés

La version initiale ne prend pas en charge les fonctionnalités suivantes :

- Définition en bloc d'objets de services
- Filtres détaillés
- Recherches
- Intégration à d'autres mécanismes d'exécution

Pour en savoir plus sur les services, reportez-vous au *Manuel d'administration*.

Nouvelle documentation pour Config Xpress

Config Xpress est un outil fourni avec CA IdentityMinder. Vous pouvez l'utiliser pour analyser et utiliser les configurations de vos environnements CA IdentityMinder.

Config Xpress vous permet d'effectuer les tâches suivantes :

- Déplacer les composants entre les environnements

  L'outil détecte automatiquement tous les autres composant requis et vous invite à les déplacer également. Cela vous permet de gagner du temps.

- Publier un rapport sur les composants système dans un fichier PDF.
- Publier la configuration XML d'un composant.

Pour plus d'informations sur l'importation de configuration, reportez-vous à la rubrique traitant de la gestion de la configuration avec Config Xpress*,* dans le *Manuel de configuration*.

Remplacement CA IdentityMinder natif pour les services de mot de passe avancés de SiteMinder

Outre les stratégies de mot de passe de base, CA IdentityMinder fournit les paramètres de mot de passe supplémentaires suivants provenant de SiteMinder :

- Expiration du mot de passe :
  - Suivi des échecs de connexion ou Suivi des connexions réussies : lorsque le suivi des échecs de connexion ou des connexions réussies est activé, ces informations sont enregistrées dans l'attribut de données de mot de passe de l'utilisateur dans le référentiel d'utilisateurs.
  - Authentifier en cas d'échec du suivi des connexions - si cette option est désactivée, les utilisateurs ne peuvent pas se connecter lorsque CA IdentityMinder ne peut enregistrer aucune information de suivi dans le référentiel d'utilisateurs.
  - Modification du mot de passe pour éviter son expiration : configure le comportement de l'expiration. Si un mot de passe n'a pas été changé après le nombre de jours spécifié, les utilisateurs sont désactivés ou sont obligés de changer leur mot de passe. Permet également d'envoyer des avertissements d'expiration pendant un nombre de jours spécifié.
  - Inactivité de mot de passe : configure le comportement des utilisateurs inactifs. Si un utilisateur ne s'est pas connecté correctement après un nombre de jours spécifié, il est désactivé ou obligé de changer son mot de passe.
  - Mot de passe incorrect : configure le nombre d'échecs de connexion permis avant la désactivation de l'utilisateur.
  - Multiple regular expressions (Plusieurs expressions régulières) : spécifie des expressions régulières auxquelles doivent correspondre ou ne pas correspondre les mots de passe. Les stratégies de mot de passe de CA IdentityMinder prennent en charge une expression unique de chaque type.
- Restrictions de mot de passe :
  - Nombre minimum de jours avant la réutilisation
  - Nombre minimum de mots de passe avant la réutilisation
  - Pourcentage de différence par rapport au dernier mot de passe
  - Ignorer la séquence lors de la vérification des différences : permet d'ignorer la position des caractères lors du calcul du pourcentage de différence.

Remarque : Cette version ne prend pas en charge les données de mot de passe historiques à partir d'un déploiement CA IdentityMinder qui utilise des services de mot de passe CA SiteMinder (historique de mots de passe) vers un déploiement qui inclut uniquement des services de mot de passe de CA IdentityMinder r12.6.

Clés dynamiques pour le chiffrement de données

Dans un environnement, vous pouvez créer des clés dynamiques qui chiffrent ou déchiffrent les données. Si vous pensez qu'un utilisateur dispose d'un accès non autorisé à une clé, vous pouvez changer le mot de passe du référentiel de clés. Le référentiel de clés est la base de données de stockage des clés secrètes. Une fois que vous changez ce mot de passe, CA IdentityMinder chiffre de nouveau les valeurs des clés.

Pour plus d'informations, consultez la section sur les clés secrètes du *Manuel d'administration*.

Synchronisation de serveur Active Directory

Vous pouvez configurer CA IAM CS pour permettre aux utilisateurs disposant d'un serveur Active Directory de synchroniser les informations d'identité locales avec les informations de terminal cloud. Par exemple, vous pouvez configurer la synchronisation du serveur AD avec une installation SalesForce basée sur le cloud. Les ajouts ou les modifications apportées à un groupe d'utilisateurs local synchronisé sont alors propagés à l'environnement SalesForce.

Cette fonctionnalité requiert CA IAM CS, un terminal pris en charge et le connecteur approprié.

Remarque sur la fonctionnalité de synchronisation d'Active Directory :

- Cette fonctionnalité prend en charge uniquement Active Directory. Aucun autre annuaire LDAP n'est pris en charge pour cette fonctionnalité dans cette version.
- Cette fonctionnalité prend uniquement en charge les terminaux basés sur le cloud pour lesquels un connecteur existe. Dans cette version, les applications prises en charge incluent Google Apps et SalesForce.

Pour plus d'informations sur cette fonctionnalité, reportez-vous au manuel *Connectors Guide*.

Audit des événements de connexion et de déconnexion

Pour améliorer la surveillance des accès utilisateur à l'environnement CA IdentityMinder, vous pouvez configurer CA IdentityMinder pour auditer les événements de connexion et de déconnexion d'utilisateur dans un environnement. Vous pouvez afficher ces événements journalisés dans le rapport de détails de l'audit par défaut.

Remarque : Vous ne pouvez pas journaliser les événements de connexion et de déconnexion d'utilisateur pour CA SiteMinder.

Vous pouvez configurer ces paramètres dans le fichier des paramètres d'audit. Pour plus d'informations sur la configuration des événements de connexion et déconnexion, consultez le chapitre Audit dans le *Manuel de configuration*.

Prise en charge SHA-2

Le hachage SHA-2 de certificat SSL est un algorithme cryptographique développé par le National Institute of Standards and Technology (NIST) et la NSA. Les certificats SHA2 sont plus sécurisés que tous les algorithmes existants auparavant. Dans CA IdentityMinder, vous pouvez configurer des certificats SSL signés en SHA-2 à la place des certificats signés avec la fonction d'hachage SHA-1.

Chapitre 2: Remarques relatives à l'installation

Ce chapitre traite des sujets suivants :

Plates-formes et versions prises en charge

CA IdentityMinder r12.6.1 inclut plusieurs changements portant sur les versions des serveurs d'applications prises en charge, les annuaires et les bases de données.

Remarque : Pour obtenir la liste complète des versions et des plates-formes prises en charge, consultez la matrice de prise en charge de CA Identity Manager sur le site de support de CA.

Composants désapprouvés et abandonnés

Certains composants sont désapprouvés, c'est-à-dire qu'ils ne seront plus pris en charge dans les futures versions. D'autres composants sont abandonnés, c'est-à-dire qu'ils ne sont plus inclus ou testés avec le produit. Ces composants sont répertoriés dans la section CA IdentityMinder Deprecation Policy sur le site de support de CA.

Conditions requises du JDK pour les installations Linux

CA IdentityMinder r12.6.1 requiert le kit de développement Java 1.6 d'Oracle.

RedHat 6.x inclut OpenJDK 1.6, qui peut entraîner le blocage indéfini du programme d'installation de CA IdentityMinder. Vérifiez que vous utilisez la version du JDK Oracle requise, comme spécifiée dans le Tableau de prise en charge de CA IdentityMinder.

Mots de passe non chiffrés

Les nouvelles installations ne chiffrent pas les mots de passe d'utilisateur par défaut. En outre, lorsque SiteMinder est intégré à CA IdentityMinder, vous ne pouvez pas activer le chiffrement de mot de passe à l'aide de l'attribut AttributeLevelEncrypt. Cet attribut fonctionne uniquement lorsque SiteMinder n'est pas installé.

Ce problème sera corrigé dans une version future.

Utilisation d'Oracle 11g R2 RAC en tant que référentiel d'utilisateurs et référentiel d'objets

Lorsque vous utilisez Oracle 11g R2 RAC comme référentiel d'utilisateurs et référentiel d'exécution, effectuez les opérations suivantes pour utiliser les fonctionnalités d'un cluster de base de données Oracle :

- Utilisez le nom SCAN (Single Client Access Name) lors de l'installation de CA IdentityMinder avec Oracle 11g R2 RAC.
- Lorsque vous créez l'espace disque logique, créez l'*espace disque logique* de la base de données sur le groupe de disques partagé.

ADAM 2008 en tant que magasin d'utilisateurs

Si vous utilisez ADAM 2008 en tant que magasin d'utilisateurs de CA IdentityMinder et que vous intégrez celui-ci à SiteMinder, vous devez installer SiteMinder r6.0 SP6/r6.x QMR6.

Echec de l'installation sur les systèmes non anglais lié aux caractères non ASCII

Pendant l'installation de CA IdentityMinder, le programme d'installation extrait les fichiers dans un répertoire temporaire. Sur certains systèmes localisés, le chemin par défaut du répertoire temporaire contient des caractères non ASCII. Par exemple, le chemin par défaut du répertoire temporaire sur un système Windows espagnol est le suivant :

C:\Documents and Settings\Administrador\Configuración local\Temp

En raison de la présence de caractères non ASCII, le programme d'installation affiche une page vide de résumé de pré-installation, ce qui entraîne l'échec de l'installation.

Solution

Modifiez la variable tmp de l'environnement afin qu'elle pointe vers un dossier contenant uniquement des caractères ASCII.

Installation de l'annuaire de provisionnement sous Linux

Si vous installez l'annuaire de provisionnement sous un système Linux, celui-ci utilise automatiquement des adresses IPv6, même si vous souhaitez utiliser IPv4. Tous les adaptateurs DSA semblent être en cours d'exécution, mais lorsque vous essayez de vous y connecter via Jxplorer ou d'installer le serveur de provisionnement, un message d'erreur indiquant un refus de connexion peut s'afficher.

Pour désactiver IPv6 sous Linux :

1. Avant l'installation de l'annuaire de provisionnement, suivez les étapes indiquées dans l'article de base de connaissances Red Hat sur la Désactivation d'IPv6 sous LINUX.
2. Assurez-vous que /etc/hosts ne possède aucune entrée pour l'adresse suivante :

   127.0.0.1 *nom_hôte*

Problèmes liés au déploiement automatique du fichier EAR de CA Identity Manager avec WebLogic

Si vous utilisez WebLogic 9 ou 10 en mode production, le fichier EAR de CA IdentityMinder ne se déploiera pas automatiquement lors du premier démarrage du serveur d'applications après une installation ou une mise à niveau. Dans ce cas, déployez iam_im.ear manuellement à partir du dossier user_projects\applications.

Contournement du pare-feu sous Windows 2008 SP2

Lors de l'installation dans des déploiements Windows 2008 SP2, le pare-feu bloque la communication avec des composants CA IdentityMinder, tels que le serveur de provisionnement, le serveur de connecteurs Java et le serveur de connecteurs C++.

Pour contourner ce problème, ajoutez des exceptions de port ou désactivez le pare-feu Windows pour accéder à des composants CA IdentityMinder distribués dans des déploiements Windows 2008 SP2.

Déploiement des pages JSP pour les actions d'administrateur

Le serveur CA IdentityMinder inclut des exemples de pages JSP pour effectuer les actions suivantes :

- Effectuer un test Ping sur le serveur principal
- Répertorier les GTM déployés
- Répertorier les informations sur les types d'objets et les fournisseurs d'objets gérés
- Répertorier les informations sur les modules d'extension
- Modifier les niveaux de journalisation

Les pages JSP sont installées dans cet emplacement :

outils_admin\samples\admin

Le dossier contient un fichier readme.txt avec des instructions pour utiliser les pages JSP.

Remarque : Vous verrez une erreur 404 si vous utilisez ces pages JSP sans suivre les instructions du fichier readme.txt.

Erreurs de connectivité CA IdentityMinder sous Linux 64 bits avec SiteMinder

Lorsque vous sélectionnez Se connecter à SiteMinder, le programme d'installation signale des erreurs avec CA Identity Manager sous Linux 64 bits. La configuration requise de l'agent dans SiteMinder n'est pas correcte.

Important : Avant de déployer un répertoire ou un environnement, suivez les étapes de correction proposée ci-dessous.

Solution

1. Prenez note du nom de l'agent et du mot de passe indiqués lors de l'installation. Vous pouvez également lire la valeur de la propriété AgentName dans le fichier suivant :

   ```
   \iam_im.ear\policyserver.rar\META-INF\ra.xml
   ```

2. Ouvrez l'interface utilisateur de SiteMinder WAM et créez un agent avec le nom de l'agent. Assurez-vous de sélectionner la case à cocher "Agent 4.x".

3. Démarrez le serveur d'applications et vérifiez qu'il n'y ait aucun problème de connectivité du serveur de stratégies.

   Une ligne sans exceptions doit apparaître comme dans l'exemple suivant :

   ```
   13:40:43, 156 WARN  [default] * Startup Step 2 : Attempting to start
   PolicyServerService
   ```

Amélioration des performances sur WebSphere et AIX

Pour une installation de WebSphere sur AIX, vous pouvez obtenir de meilleures performances dans la console d'utilisateur en définissant la taille de segment de mémoire maximum.

Procédez comme suit:

1. Recherchez le fichier server.xml à l'emplacement suivant :
   `WAS_HOME/profiles/`*`profil`*`/config/cells/`*`cellule`*`/nodes/`*`noeud`*`/servers/`*`serveur`*

2. Ajoutez maximumHeapSize="1000" à l'élément jvmEntries.

   Vous pouvez utiliser une valeur plus élevée si nécessaire. Par exemple, pour définir l'élément maximumHeapSize sur 2 Go (2048 Mo), vous l'ajoutez comme affiché en gras dans l'extrait du fichier suivant :

```
<jvmEntries xmi:id="JavaVirtualMachine_1183122130078"
verboseModeClass="false"
   verboseModeGarbageCollection="false" maximumHeapSize="2048"
verboseModeJNI="false" runHProf="false" hprofArguments=""
debugMode="false"
debugArgs="-agentlib:jdwp=transport=dt_socket,server=y,suspend=
n,address=7777" genericJvmArguments="">
      <systemProperties xmi:id="Property_1"
name="com.ibm.security.jgss.debug" value="off"
required="false"/>
      <systemProperties xmi:id="Property_2"
name="com.ibm.security.krb5.Krb5Debug" value="off"
required="false"/>
    </jvmEntries>
```

Omission des erreurs WebSphere 7Oracle

Lorsque CA IdentityMinder est installé à l'aide d'un référentiel d'exécution Oracle et du JRE WebSphere 7 par défaut, l'erreur suivante s'affiche dans les journaux CA IdentityMinder.

> Oracle does not support the use of version 10 of their JDBC driver with the version of the Java runtime environment that is used by the application server. (Oracle ne prend pas en charge l'utilisation de la version 10 du pilote JDBC avec la version du JRE utilisée par le serveur d'applications.)

Vous pouvez ignorer cette erreur.

Chapitre 3: Mises à niveau

Les problèmes de mise à niveau suivants ont été détectés dans CA IdentityMinder r12.5 SP1.

Ce chapitre traite des sujets suivants :

Chemins de mise à niveau pris en charge

Vous pouvez réaliser une mise à niveau vers CA IdentityMinder r12.6.1 à partir des versions suivantes :

- CA Identity Manager r12
- CA Identity Manager r12.5
- CA Identity Manager r12.5 SPx
- CA IdentityMinder r12.6

Si vous avez une version antérieure à CA Identity Manager r12, procédez d'abord à la mise à niveau vers la version 12, 12.5 ou l'une des versions comprises entre 12.5 SP1 et 12.5 SP6. Ces versions incluent l'outil imsconfig, qui est requis pour mettre à niveau une version antérieure à la version 12. Vous pouvez ensuite procéder à la mise à niveau vers CA IdentityMinder r12.6.1.

Nouveau fichier de définition de rôle Active Directory

Assurez-vous que vous importez le nouveau fichier de définition de rôle pour Active Directory dans chaque environnement. L'environnement CA IdentityMinder actuel peut avoir une version antérieure du fichier de définition de rôle Active Directory. Importez le fichier pour mettre à niveau les définitions de rôle vers la version 1.08. Pour plus d'informations sur l'importation de fichiers de définition de rôle, suivez les procédures du manuel *Upgrade Guide*.

Mise à jour du fichier jboss.xml

Lors du redémarrage de JBoss ou de l'initialisation de CA IdentityMinder, plusieurs messages d'erreurs sont journalisés dans le fichier server.log de CA IdentityMinder. Ces messages sont associés à des événements gérés par JMX, mais le bean de message récepteur n'est pas encore initialisé. Pour corriger ce problème, le fichier suivant inclut désormais une clause depends :

```
iam_im.ear\iam_im_identityminder_ejb.jar\META-INF\jboss.xml
```

La clause dépends est incluse dans cette section :

```
<message-driven>
<ejb-name>SubscriberMessageEJB</ejb-name>
<destination-jndi-name>queue/iam/im/jms/queue/com.netegrity.ims.ms
g.queue
</destination-jndi-name>
<depends>jboss.web.deployment:war=/iam/im</depends>
</message-driven>
```

Assurez-vous d'inclure cette section dans le fichier jboss.xml. Une fois incluse, le bean de message récepteur est initialisé avant que JMX démarre le traitement de la file d'attente d'événements.

Serveurs d'applications 64 bits

CA IdentityMinder r12.6.1 prend en charge les serveurs d'applications 64 bits, qui fournissent de meilleures performances que les serveurs d'applications 32 bits. Les versions de serveur d'applications 64 bits suivantes sont prises en charge :

- JBoss 5.0 and 5.1 Enterprise Application Platform (EAP)
- JBoss 5.1 Open Source
- Oracle WebLogic 11g (10.3.5)
- IBM WebSphere 7.0

Si CA Identity Manager s'exécute actuellement sur la version 64 bits de l'un de ces serveurs d'applications, vous pouvez procéder à la mise à niveau vers CA IdentityMinder r12.6.1 en suivant la procédure décrite dans le manuel *Upgrade Guide.*

Si CA Identity Manager s'exécute actuellement sur une version inférieure ou une version 32 bits du serveur d'applications, désinstallez CA Identity Manager et installez CA IdentityMinder sur le nouveau serveur d'applications. Ce processus est appelé migration.

Pour obtenir des détails complets sur la mise à niveau et la migration, consultez le manuel *Upgrade Guide*.

Problème de mise à niveau de clusters à partir de CA IdentityMinder r12 CR6 (ou version ultérieure)

Si vous mettez un cluster à niveau à partir de CA IdentityMinder r12 CR6 (ou version ultérieure) vers CA IdentityMinder r12.5 SP1, il se peut que la mise à niveau échoue suite à l'effacement de certaines propriétés du cluster dans le fichier d'installation.

Solution

Avant d'effectuer la mise à niveau, vérifiez que les propriétés suivantes figurent dans le fichier im-installer.properties :

- WebSphere : vérifiez si le nom du cluster est rempli dans DEFAULT_WAS_CLUSTER. Si ce nom est manquant, rajoutez-le manuellement.
- WebLogic : vérifiez si le nom du cluster est rempli dans DEFAULT_BEA_CLUSTER. Si ce nom est manquant, rajoutez-le manuellement.

Remarque : Ce problème ne concerne pas les clusters JBoss.

Par défaut, le fichier d'installation se trouve aux emplacements suivants :

- Windows : C:\Program Files\CA\CA Identity Manager\install_config_info\im-installer.properties
- Unix : /opt/CA/CA_Identity_Manager/install_config_info/im-installer.properties

Mise à niveau de CA Identity Manager r12.5 SP6 ou d'une version antérieure sur WebLogic

Symptôme :

Si vous procédez à la mise à niveau à partir de la version 12.5 SP6 ou d'une version antérieure sur le serveur d'applications WebLogic, l'erreur suivante s'affiche au démarrage du flux de travaux :

```
WARN  [ims.default] * Startup Step 25 : Attempting to start SchedulerService
ERROR [ims.bootstrap.Main] The IAM FW Startup was not successful
ERROR [ims.bootstrap.Main] org.quartz.SchedulerException: JobStore class
'org.quartz.impl.jdbcjobstore.JobStoreCMT' props could not be configured.
[See nested exception: java.lang.NoSuchMethodException: No setter for
property 'lockHandler.class']
```

Solution :

1. Arrêtez WebLogic
2. Accédez au dossier <IAM-EAR>/APP-INF/lib.
3. Renommez les fichiers suivants :
   - common-pool-1.3.jar
   - annotations.jar
   - eurekifyclient.jar
   - quartz-all-1.5.2.jar
4. Lancez le serveur d'applications.
5. L'erreur au démarrage du flux de travaux ne s'affiche plus.

Erreur de migration d'environnement

Symptôme :

Lors d'une mise à niveau à partir de CA IdentityMinder r12 CR1/CR2/CR3, il se peut que le message d'erreur suivant apparaisse lors de l'importation des environnements :

Attribute "accumulateroleeventsenabled" is not allowed to appear in element "Provisioning". (L'affichage de l'attribut accumulateroleeventsenabled n'est pas autorisé dans l'élément Provisionnement.)

Solution :

Dans le zip exporté Env.zip, ouvrez le fichier envsettings.xml et mettez à jour "accumulateroleeventsenabled" en supprimant le deuxième "c" dans "accumulate" : acumulateroleeventsenabled.

Erreur de mise à niveau du fournisseur d'informations d'identification

Après avoir mis à niveau le fournisseur d'informations d'identification de CA IdentityMinder r12 sur une plate-forme Windows 32 bits, la case à cocher Désactiver Microsoft Password Credential Provider est désactivée dans l'application CAIMCredProvConfig.

Solution

Ouvrez l'application CAIMCredProvConfig et sélectionnez la case à cocher.

Erreur interne du fournisseur d'informations d'identification Vista

Symptôme :

Lorsque je mets à niveau le fournisseur d'informations d'identification Vista de CA IdentityMinder sur des plates-formes Windows 64 bits, je reçois le message *Erreur interne 2324.2.*

Solution :

Aucune action n'est requise, car le processus de mise à niveau s'est déroulé correctement.

Absence de fenêtre de recherche avec la tâche d'exploration et de corrélation

Si vous avez effectué la mise à niveau à partir de CA IdentityMinder r12 *ou* de CA IdentityMinder r12.5 *et* que vous avez migré la tâche d'exploration et de corrélation vers le nouveau modèle de récurrence, le bouton Parcourir ne fonctionne pas correctement.

Solution

Configurez une fenêtre de recherche pour cette tâche, afin qu'une fenêtre de recherche s'affiche lorsque vous cliquez sur le nouveau bouton Parcourir.

Erreur non irrécupérable après la mise à niveau du gestionnaire de provisionnement depuis r12

Symptôme :

Après avoir mis à niveau le gestionnaire de provisionnement depuis CA IdentityMinder r12 CRx, le programme d'installation affiche le message suivant :

```
L'assistant d'installation a terminé la mise à niveau de CA Identity
Manager, mais des erreurs non fatales ou des avertissements se sont
produits pendant l'opération. Pour plus d'informations, reportez-vous
au journal d'installation sous C:\Program Files\CA\CA Identity
Manager.
Des erreurs ou des avertissements ont été signalés au niveau des
composants suivants
```

Le journal d'installation de CA IdentityMinder contient l'entrée suivante :

```
Install, com.installshield.product.actions.Files, err,
ServiceException: (error code = -30016; message = "Impossible
d'accéder au fichier car celui-ci est utilisé par un autre processus."
```

Solution :

L'erreur se produit parce que le programme d'installation ne peut pas créer un répertoire qui existe. Toutefois, l'installation s'est déroulée correctement et le gestionnaire de provisionnement est entièrement fonctionnel.

Renommage des terminaux ACF2, RACF et TSS avant la mise à niveau

Les espaces dans les noms de terminaux ne sont plus pris en charge. Si vous avez créé des terminaux dont les noms contiennent des espaces dans une version précédente, supprimez les espaces avant de procéder à la mise à niveau vers la version 12.6.

Chapitre 4: Problèmes connus

Ce chapitre traite des sujets suivants :

Général

Plusieurs problèmes généraux ont été détectés dans CA IdentityMinder r12.5 SP1.

Echec de la création de l'annuaire de provisionnement via la console de gestion

Lors de la création d'un annuaire de provisionnement via la console de gestion, le champ de nom de domaine du serveur de provisionnement ne permet pas l'utilisation de caractères de langue étrangères. Le message d'erreur suivant peut s'afficher :

“could not connect to the LDAP server machinename:20389 with userDN etGlobalUserName=admin,eTGlobalUserContainerName:GlobalUsers,eTNamespacename=CommonObjects,dc=foreignChars, dc=eta and specified password.”

AttributeLevelEncryption pour les mots de passe d'utilisateur

Lorsque vous spécifiez la classification de données AttributeLevelEncryption pour les attributs du fichier de configuration d'annuaire (directory.xml), CA IdentityMinder chiffre la valeur d'attribut dans le référentiel d'utilisateurs. Dans la console d'utilisateur, la valeur s'affiche en texte clair.

La description d'attribut suivante affiche la classification des données AttributeLevelEncryption :

```
<ImsManagedObjectAttr physicalname="title" description="Title"
displayname="Title" valuetype="String" maxlength="0"
searchable="false">

<DataClassification name="AttributeLevelEncrypt"/>

</ImsManagedObjectAttr>
```

Dans les environnements avec la configuration suivante, l'activation du chiffrement de niveau attribut pour les mots de passe empêche les utilisateurs de se connecter :

- CA IdentityMinder est intégré à CA SiteMinder et
- le référentiel d'utilisateurs est une base de données relationnelles.

Dans cette version, la classification de données AttributeLevelEncryption est supprimée de l'attribut de mot de passe dans les fichiers de configuration d'annuaire (directory.xml) suivants :

- DirectoryTemplates/RelationalDatabase.xml
- fwSampleRDB.xml
- Samples/NeteAutoRDB/NoOrganization.xml
- Samples/NeteAutoRDB/Organization.xml

Ces fichiers se trouvent dans le répertoire *outils_admin*.

Remarque : Pour plus d'informations sur la gestion des attributs sensibles, reportez-vous au *Manuel de configuration*.

Spécification de nom unique LDAP lors de l'utilisation du service Web d'exécution des tâches

Symptôme :

Lors de l'utilisation du service Web d'exécution des tâches pour appeler la tâche CreateOracleServerAccountTemplate, vous pouvez obtenir le message d'erreur suivant :

```
Message d'erreur : <code>500</code>

<description>Echec de l'exécution de CreateOracleServerAccountTemplate. Erreur

Message : com.ca.iam.model.IAMParseException: Not a valid IAM handle:

'UHGUSERS' ProcessStep::Unknown TabName: null ERRORLEVEL::Fatal</description>
```

Le problème est que le nom unique que le service Web d'exécution des tâches attend ne correspond pas à celui de l'annuaire de provisionnement.

Cet exemple n'a pas fonctionné :

```
eTORADirectoryName=WSDLOracle4,eTNamespaceName=Oracle Server,dc=im,dc=eta
```

Cet exemple est le nom unique qui n'a pas fonctionné :

```
EndPoint=WSDLOracle4,Namespace=Oracle Server,Domain=im,Server=Server
```

Solution :

Pour rechercher le mappage, vérifiez que les niveaux de journalisation du serveur d'applications sont définis sur le mode détaillé. Exécutez les tâches du gestionnaire d'identité pour lesquelles vous avez besoin des donnée/chemins d'accès. Les chemins d'accès se trouvent dans le fichier journal. Recherchez < et insert into IM_ peut être utile pour obtenir les chemins d'accès et les valeurs d'attribut transférées par les tâches.

Echec de la commande setpasswd sur les systèmes Linux 64 bits

Symptôme :

Sur les systèmes Linux 64 bits et Solaris, un échec de la commande setpasswd se produit avec l'erreur :

```
"/opt/CA/SharedComponents/csutils/bin/expect: error while loading shared libraries:
libtcl8.4.so: cannot open shared object file: No such file or directory"
```

Solution :

Définissez LD_LIBRARY_PATH sur la valeur :

/opt/CA/SharedComponents/csutils/lib/tcl8.4

La commande setpasswd ne génère plus cette erreur.

Problème avec la stratégie de mot de passe lors de l'utilisation d'une combinaison du référentiel d'utilisateurs et de l'annuaire de provisionnement

Symptôme :

CA IdentityMinder n'applique pas certaines stratégies de mot de passe dans les déploiements qui utilisent une combinaison du référentiel d'utilisateurs combiné et de l'annuaire de provisionnement. Ce problème se produit avec des stratégies de mot de passe qui incluent les règles et les restrictions suivantes :

- Expiration du mot de passe :
  - Suivi des échecs de connexion ou des connexions établies
  - Authentification d'une connexion
  - Expiration du mot de passe s'il n'est pas modifié
  - Inactivité du mot de passe
  - Mot de passe incorrect
  - Plusieurs expressions régulières
- Restrictions de mot de passe :
  - Nombre minimum de jours avant la réutilisation
  - Nombre minimum de mots de passe avant la réutilisation
  - Pourcentage de différence par rapport au dernier mot de passe
  - Omission de séquence lors de la vérification des différences

Ce problème se produit parce que %PASSWORD_DATA% est mappé vers un attribut binaire plutôt qu'un attribut de chaîne par défaut.

Solution :

Dans la console de gestion, mappez %PASSWORD_DATA% vers un attribut eTCustomField qui n'est pas mappé vers aucun autre attribut. Par exemple, eTCustomField99.

Après avoir mis à jour le mappage, redémarrez l'environnement.

Remarque : Pour plus d'informations sur la mise à jour d'un annuaire CA IdentityMinder existant, consultez le *Manuel de configuration*.

Connexion impossible au serveur CA IdentityMinder lors de la configuration de l'agent de synchronisation de mots de passe Active Directory 64 bits

Symptôme :

Lors de la configuration de l'agent de synchronisation de mots de passe 64 bits, la connexion au serveur CA IdentityMinder pour récupérer la liste des terminaux Active Directory disponibles est impossible.

Solution :

Vous pouvez configurer uniquement les chiffrements que CA IAM CS utilise. Ajoutez les trois nouveaux chiffrements FIPS SSL à la suite du chiffrement utilisé par CA IAM CS.

Procédez comme suit:

1. Ouvrez le fichier de configuration suivant dans un éditeur de texte :

   ```
   cs_home\jcs\conf\server_osgi_shared.xml
   ```

2. Recherchez la propriété defaultCipherSuite dans le fichier. Exemple de code dans le fichier :

   ```
   <property
   name="defaultCipherSuite"><value>FIPS_TLS_PLUS_SSL_Ciphers</value></property>
   <property name="cipherSuites">
               <map>
                   <entry key="FIPS_TLS_PLUS_SSL_Ciphers">
                       <list>
                           <value>TLS_RSA_WITH_AES_128_CBC_SHA</value>
                           <value>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</value>
                           <value>TLS_DHE_DSS_WITH_AES_128_CBC_SHA</value>
                         </list>
   ```

   Dans cet exemple, *FIPS_TLS_PLUS_SSL_Ciphers* est la suite par défaut qui correspond à la liste des chiffrements sous la propriété cipherSuites.

3. Ajoutez les entrées suivantes à la liste :

   ```
   <value>SSL_RSA_WITH_3DES_EDE_CBC_SHA</value>
   <value>SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA</value>
   <value>SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA</value>
   ```

4. Cliquez sur Enregistrer.

5. Redémarrez le service CA IAM CS.

   L'agent de synchronisation de mots de passe d'annuaire 64 bits actif se connecte désormais sans erreur.

L'outil de résolution de participants de flux de travaux échoue pour EnableUserEventRoles

Symptôme :

Lorsque vous essayez de changer les paramètres de flux de travaux pour la tâche, vous pouvez voir ce message :

```
Impossible de définir l'objet principal de la tâche dans la section de description de l'outil de résolution {0} pour la tâche de sélection multiple.
```

Solution :

Accédez à la page de flux de travaux et définissez l'approbateur sur Objet associé à l'événement.

Nom dupliqué dans Afficher les tâches soumises

Symptôme :

Dans certains environnements de haute disponibilité à charges lourdes, le serveur CA IdentityMinder peut envoyer des demandes parallèles au serveur de provisionnement et introduire des conditions de course dans le serveur de provisionnement lors du traitement de demandes de modification parallèles sur le même utilisateur global.

Solution :

Définissez le paramètre de gestionnaire de provisionnement suivant sur Non et redémarrez le serveur de provisionnement.

```
Serveur Identity Manager : autoriser les modifications simultanées sur le même utilisateur global
```

Remarque : En cas de sorties de programme lors de l'accès aux utilisateurs globaux, laissez ce paramètre défini sur Oui.

Message d'erreur Introuvable lors de la création d'un environnement dans certains déploiements

Si CA IdentityMinder est intégré à CA SiteMinder 6.0.5 CR 31 (ou version ultérieure), il se peut qu'un message d'erreur (Erreur 404 - Introuvable) apparaisse lors des tentatives d'accès à l'URL d'un nouvel environnement.

Cela est dû à un problème de mise en cache dans le serveur de stratégies.

Solution

Pour résoudre ce problème, procédez comme suit :

Windows :

1. Ajoutez un mot clé au registre SiteMinder comme indiqué ci-dessous :
   a. Accédez à \\HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\Siteminder\CurrentVersion\ObjectStore.
   b. Ajoutez la clé ServerCmdMsec avec les paramètres suivants :
      - Type : DWORD
      - Valeur : 1
   c. Relancez le serveur de stratégies.
2. Redémarrez le serveur d'applications.
3. Fermez toutes les instances du navigateur, puis utilisez une nouvelle instance pour accéder à l'URL de l'environnement.

Solaris :

1. Ajoutez une ligne au fichier <CA_HOME folder>/netegrity/siteminder/registry/sm.registry.
   ServerCmdMsec= 0x1 REG_DWORD
2. Redémarrez le serveur de stratégies.
3. Redémarrez le serveur d'applications.
4. Fermez toutes les instances du navigateur, puis utilisez une nouvelle instance pour accéder à l'URL de l'environnement.

Modification d'attributs composés à valeur unique dans CA Identity Manager

Si vous modifiez un attribut composé à valeur unique dans CA IdentityMinder pour un terminal dynamique, veillez à spécifier une seule valeur. Si vous spécifiez plusieurs valeurs, la valeur actuelle sera effacée et aucune valeur ne sera appliquée à l'attribut. Ce problème n'affecte pas le gestionnaire de provisionnement.

Limitations du chargeur en bloc dans le niveau d'attribut de relation

Le chargeur en bloc ne peut pas mettre à jour les opérations de tâche sur les objets d'utilisateur dans le niveau d'attribut de relation.

- Les attributs de relation qui ne sont pas mis à jour par le chargeur en bloc sont les rôles d'accès d'utilisateurs, les rôles d'administration d'utilisateurs, les rôles de provisionnement d'utilisateurs, l'appartenance des utilisateurs au groupe et le groupe Groupes.
- Les attributs de relation qui sont écrasés lorsque vous remplacez les anciennes valeurs d'attribut par de nouvelles à partir du fichier de chargeur en bloc sont les attributs d'administrateurs de groupes et les attributs personnalisés ou à valeurs multiples par défaut.

Erreur au moment de créer l'environnement compatible avec le provisionnement à l'aide du modèle à jetons

Dans ce cas, CA IdentityMinder ne peut pas affecter le rôle Provisionnement du gestionnaire de synchronisations à l'administrateur entrant défini dans l'assistant de création d'environnement.

Si le modèle d'environnement comporte des jetons ou des chaînes traduites pour le nom du rôle Provisionnement du gestionnaire de synchronisations, la recherche échoue et NoSuchObjectException survient.

Conditions préalables pour les applications Oracle

Vous devez définir NLS_LANG comme variable d'environnement système, avec la valeur .UTF8.

Remarque : Il doit y avoir un point (.) devant UTF8 sur le système où le serveur de connecteurs est installé.

Magasin d'utilisateurs Oracle 11gR2 RAC : la recherche est sensible à la casse

Symptôme :

Lorsque Oracle 11gR2 RAC est le magasin d'utilisateurs, la recherche d'utilisateurs, de groupes ou d'organisations ne fournit parfois aucun résultat bien que les objets existent.

Solution :

Pour ce magasin d'utilisateurs, la recherche est sensible à la casse. Par exemple, la recherche sur *smith* ne renvoie aucun résultat si l'utilisateur a été créé sous la forme *Smith* dans la base de données. Utilisez la même casse que celle utilisée lorsque l'objet a été créé dans la base de données.

Reconnexion impossible à Oracle lors de l'utilisation de CA IdentityMinder sur JBoss

Symptôme :

Lorsque vous utilisez JBoss 5.x avec une source de données de base de données Oracle et procédez à la mise à niveau de CA IdentityMinder à partir d'une version 12.5, une interruption de l'application se produit si le serveur de base de données est redémarré. L'interruption est causée par JBoss lors du remplacement de la propriété background-validation-minutes par background-validation-millis.

Solution :

Pour résoudre ce problème, procédez comme suit :

1. Arrêtez le serveur d'applications.
2. Ouvrez les fichiers de source de données sous */jboss folder/server/default [or server name in cluster]/deploy* et supprimez la ligne suivante :

   <background-validation-minutes> </background-validation-minutes>
3. Ajoutez la ligne suivante :

   <background-validation-millis>120000</background-validation-millis>

   Remarque : 120000 est l'équivalent des 2 minutes spécifiées préalablement par défaut pour background-validation-minutes. Configurez la valeur selon les besoins métier.
4. Redémarrez le serveur d'applications.

Remarque : Le problème n'affecte pas les nouvelles installations de CA IdentityMinder.

Echec du passage au contenu principal dans Mozilla FireFox

Symptôme :

Un lien Passer directement au contenu principal s'affiche dans la partie supérieure de la console d'utilisateur. Ce lien déplace la trame principale affichée en haut de la page. Toutefois, un échec du lien se produit dans Mozilla FireFox.

Solution :

Pour prendre en charge cette fonctionnalité, utilisez Microsoft Internet Explorer 8 ou une version ultérieure avec JAWS.

Echec des modifications simultanées apportées à un utilisateur

Un échec d'une tâche Modifier un utilisateur se produit dans ces situations :

- Si vous essayez de désactiver un utilisateur pendant que vous le modifiez, un échec de la tâche se produit.
- Si vous ajoutez l'attribut forcePasswordChange à la fenêtre Profil de l'utilisateur pendant que vous le modifiez, un échec de la tâche se produit.

Modification de la syntaxe Policy Xpress

Symptôme :

A cause d'une modification apportée à la syntaxe Policy Xpress, une erreur peut se produire. Elle se produit si la stratégie utilise l'analyse de chaîne pour l'identificateur de compte et que l'utilisateur a plusieurs comptes sur un terminal d'un seul niveau. Les terminaux Oracle, OS400 et Microsoft SQL ont des comptes qui servent de conteneur virtuel, placés sous le nom du terminal. A partir de la version 12.6.1, la syntaxe de l'identificateur de compte est la suivante :

- Pour les connecteurs à un seul niveau, EndpointName:EndpointName:AccountName
- Pour les connecteurs hiérarchiques, EndpointName:AccountContainerPath:AccountName

Solution :

Recherchez les stratégies Policy Xpress qui utilisent l'analyse de chaîne pour l'identificateur de compte. Mettez à jour ces stratégies de façon à ce qu'elles soient conformes à la nouvelle syntaxe.

Mise à jour de la rubrique d'Aide SAP

L'Aide pour l'onglet Paramètres par défaut relatif aux comptes SAP r3 doit avoir cette définition pour la notation décimale.

- Spécifie les différents modes de représentation des notations décimales.
- Vous avez le choix entre les options ci-dessous.

  1.234.567,89

  1,234,567.89

  1 234567,89

Génération de rapport

Les problèmes de génération de rapport suivants ont été détectés dans CA IdentityMinder r12.5 SP1.

Respect de la casse obligatoire pour les recherches de filtre d'utilisateur dans les fichiers XML de clichés personnalisés de comptes d'utilisateurs et de comptes de terminal

Symptôme

Lorsque vous créez un filtre sur %USER_ID% dans les éléments d'exportation *useraccounts* des fichiers XML de clichés personnalisés des *comptes d'utilisateur*et des *comptes de terminal,* le rapport n'affiche pas les résultats bien que l'utilisateur existe.

Solution

La recherche de filtre doit respecter la casse.

Satisfy=All ne fonctionne pas correctement dans le fichier XML

Dans un fichier XML de paramètres de cliché, satisfy=all et satisfy=any se comportent tous les deux de la même façon que satisfy=any (similaire à l'opérateur OR).

Problème lors de l'utilisation de plusieurs filtres avec l'objet de terminal

Symptôme :

Lorsqu'une définition de cliché est créée avec l'objet de terminal à l'aide de plusieurs filtres, aucune donnée du terminal n'est capturée.

Solution :

Dans l'onglet Stratégies de clichés, au lieu de sélectionner plusieurs objets de terminal, entrez un astérisque (*) pour sélectionner plusieurs objets de terminal.

Impossible de capturer les données d'objet de groupe dans un cliché

Symptôme :

Lorsqu'une définition de cliché est créée avec un objet de groupe à l'aide du filtre org-filter, aucune donnée du groupe n'est capturée.

Solution :

Dans l'onglet Stratégies de clichés, au lieu de sélectionner org-filter dans la liste déroulante, sélectionnez (Tout).

Général

Plusieurs problèmes généraux de provisionnement ont été détectés dans CA IdentityMinder r12.5 SP1.

Renommage des rôles de provisionnement non prise en charge

Le renommage des rôles de provisionnement après leur création n'est pas pris en charge.

Performances du serveur de provisionnement affectées par le dépassement du niveau INFO lors d'opérations de journalisation Solaris ECS

En cas de dépassement du niveau INFO lors d'opérations de journalisation Solaris ECS, les informations sont journalisées avant l'envoi d'une réponse, ce qui pour a effet de retarder votre demande pendant l'écriture du journal.

Solution

Si les performances du serveur de provisionnement sont ralenties, arrêtez la journalisation Solaris ECS.

Erreurs signalant des terminaux existants lors de l'ajout d'un terminal

Si vous supprimez un terminal avant d'en ajouter un portant le même nom, le serveur de provisionnement signale parfois un échec en indiquant qu'un terminal portant ce nom existe déjà. Cela peut se produire lorsque vous configurez de multiples serveurs de connecteurs pour gérer ce terminal. Cet échec est lié à un problème de suppression du terminal, car la notification de suppression n'est pas envoyée à tous les serveurs de connecteurs.

Solution

Redémarrez tous les serveurs de connecteurs configurés pour gérer le terminal.

Echec de la corrélation d'un terminal Microsoft SQL

Symptôme :

Un échec de la corrélation d'un terminal Microsoft SQL se produit avec le message suivant :
`Object MS SQL Logins global users creation failed (Echec de la création des connexions d'objet MS SQL pour les utilisateurs globaux). Unable to determine object class from distinguished name (Impossible de déterminer la classe d'objet à partir du nom unique).`

Cette erreur se produit lorsque tous les conteneurs sont sélectionnés pour un terminal Microsoft SQL, pas seulement le conteneur avec des comptes.

Solution :

1. Créez une définition d'exploration et de corrélation, et recherchez un terminal Microsoft SQL.
2. Recherchez tous les conteneurs, mais sélectionnez uniquement le *nom de terminal* comme conteneur.
3. Sélectionnez les attributs d'exploration et de corrélation.
4. Exécutez la définition d'exploration et de corrélation.

Limitation liée au nom de connexion SiteMinder pour le nom d'utilisateur global

Les chaînes de caractères ou caractères suivants ne peuvent pas figurer dans un nom d'utilisateur global si cet utilisateur doit se connecter au serveur de stratégies SiteMinder :

&
*
:
( )

Solution

N'utilisez pas ces caractères dans les noms d'utilisateurs globaux.

CA IAM CS et Connector Xpress

Les problèmes suivants sont liés au serveur de connecteurs CA IAM (CA IAM CS) et à Connector Xpress.

Remarque : Dans CA IdentityMinder 12.6, le serveur de connecteurs Java (JCS) a été renommé serveur de connecteurs CA IAM (CA IAM CS).

Fenêtre de gestion des comptes JNDI : échec de la création de comptes contenant de multiples classes d'objets structurels

Vous ne pouvez pas créer de comptes contenant plusieurs classes d'objets structurels.

Types de terminaux

Plusieurs problèmes de gestion des types de terminaux ont été détectés dans CA IdentityMinder r12.5 SP1.

Général

Les sections suivantes décrivent les problèmes connus pour les différents connecteurs.

Configuration des terminaux avec verrouillage automatique du nombre de tentatives et définition d'un nombre maximum suffisant de tentatives

Certains terminaux disposent d'un système de verrouillage automatique du nombre N de tentatives. Vous devez donc configurer les comptes de connexion aux terminaux utilisant le serveur de connecteurs Java pour que ce nombre N soit suffisant, voire illimité, car les tentatives de connexion du serveur de connecteurs Java s'épuisent rapidement.

Si le compte est verrouillé en mode natif en raison d'un nombre N trop important de tentatives, vous devrez peut-être utiliser des outils natifs pour le déverrouiller avant de pouvoir obtenir de nouveau le terminal. Tout dépend du comportement natif exact de verrouillage du terminal.

Erreur dans les fenêtres de recherche de terminal après la mise à niveau à partir de 12.5 SP6 ou d'une version antérieure

Symptôme :

Une erreur ressemblant au message suivant se produit lorsque vous importez des fichiers de définitions de rôle de terminal à partir de la version 12.5 SP6 ou d'une version antérieure, vers la version 12.5 SP7 ou une version ultérieure :

"Error in screen definition "Default Endpoint Type Primary Group Endpoint Capability Search" with tag "DefaultActiveDirectoryPrimaryGroupEndpointCapabilitySearch" Error: The type "UNKNOWN" is not a valid object type." (Erreur dans la définition de fenêtre Groupe Terminal par défaut - Recherche des capacités de terminaux avec la balise DefaultActiveDirectoryPrimaryGroupEndpointCapabilitySearch. Erreur : de balise : Le type UNKNOWN n'est pas un type d'objet valide.)

Dans CA Identity Manager r12.5 SP7, certains objets ont été renommés. Ces objets sont référencés dans les fenêtres de recherche de capacité de terminal. Après avoir procédé à la mise à niveau vers la version 12.5 SP7 ou ultérieure, une erreur peut se produire lorsque vous importez des fichiers de définitions de rôle incluant des fenêtres qui référencent les anciens noms d'objet.

Ce problème a été identifié dans les terminaux Active Directory et CA Access Control.

Considérez l'exemple de terminal Active Directory suivant :

Dans CA Identity Manager r12.5 SP6, le nom de fenêtre de recherche de capacité de terminal Active Directory a référencé l'objet ACTIVEDIRECTORY_ADUNIXPRIMARYGROUP'.

Le nom d'objet s'affiche dans la définition de fenêtre suivante :

```
<Screen name="Groupe Active Directory par défaut - Recherche des capacités de terminaux"
tag="DefaultActiveDirectoryPrimaryGroupEndpointCapabilitySearch"

screendefinition="EndpointCapabilitySearch"

Object="ACTIVEDIRECTORY_ADUNIXPRIMARYGROUP">
```

Dans CA Identity Manager r12.5 SP7, le nom d'objet a été remplacé par ACTIVEDIRECTORY_ETADSGROUP.

Le nouveau nom d'objet s'affiche dans la définition de fenêtre suivante :

```
<Screen name="Groupe Active Directory par défaut - Recherche des capacités de terminaux"

tag="DefaultActiveDirectoryGroupEndpointCapabilitySearch"

screendefinition="EndpointCapabilitySearch"

object="ACTIVEDIRECTORY_ETADSGROUP">
```

Solution :

Supprimez les définitions de fenêtre qui référencent l'ancien nom d'objet avant d'importer un fichier de définitions de rôle.

Problèmes de synchronisation des comptes et des modèles de comptes dans les tâches de création ou de modification de la console d'utilisateur

Symptôme :

La synchronisation des comptes explicites n'est pas prise en charge dans la console d'utilisateur.

Solution :

Pour synchroniser les comptes avec les modèles de comptes, utilisez le gestionnaire de provisionnement.

Echec lié à la modification directe du terminal lors de l'importation entre le terminal et le serveur de provisionnement

La modification directe du terminal (sans utiliser le serveur de provisionnement) renvoie un message d'erreur lors de l'importation due à l'incohérence des données entre le terminal et le serveur de provisionnement. Voici deux exemples :

- Un utilisateur a supprimé des tables du terminal MSSQL à l'aide des outils natifs, et en conséquence, certains utilisateurs reçoivent des ressources qui n'existent plus.

  Pour résoudre cette erreur, explorez de nouveau le terminal à l'aide du serveur de provisionnement.

- Un utilisateur a supprimé certains rôles de serveur sur le terminal et les modèles de compte auxquels ces rôles étaient affectés ont reçu des rôles supplémentaires qui n'existent plus sur le terminal.

  Pour résoudre ce problème, supprimez manuellement ces rôles de serveur qui ont été supprimés des modèles de comptes.

Restrictions sur le nom de terminal pour les connecteurs ACF2 ACFESAGE, RACF IRRDBU00 et TSSCFILE

Symptôme :

Créer un terminal avec le nom user test, “user-test” et “_usertest” sur des connecteurs de fichier de vidage entraîne un échec avec le message : Cannot create pool able connection factory (Impossible de créer un sous-objet de connexion pouvant être mis en pool).

Solution :

Les caractères d'espace ne sont plus permis dans les noms de terminaux pour les connecteurs ACF2 ACFESAGE, TSSCFILE ou RACF IRRDBU00. Les restrictions suivantes s'appliquent également au nom de terminal des connecteurs :

- Doit contenir entre 1 et 30 caractères.
- Doit commencer par des caractères alphanumériques.
- Doit contenir uniquement des caractères alphanumériques et/ou des traits de soulignement.

Avant de procéder à la mise à niveau vers cette version, supprimez les terminaux de fichier de vidage de mainframe existants qui ne sont pas conformes aux restrictions spécifiées.

Contrôle d'accès

Texte des boutons de la fenêtre de calendrier affichés en anglais

Lorsque vous créez un modèle de compte dans le terminal CA Access Control, les boutons OK et Cancel dans la fenêtre de calendrier s'affichent en anglais dans l'onglet Connexion.

Suppression de groupes d'un compte CA Access Control

Symptôme :

Lorsque vous supprimez un groupe natif d'un compte d'utilisateur natif provisionné par le connecteur CA Access Control, les groupes natifs sont supprimés en deux étapes. Ce processus supprime toutes les appartenances au groupe existantes, puis rajoute toutes les appartenances au groupe requises. L'appartenance au groupe appropriée est définie pour le compte, mais cela peut engendrer des problématiques opérationnelles pour certains clients.

Solution :

Si vous ne voulez pas utiliser ce processus en deux étapes, vous pouvez utiliser Connector Xpress pour créer une définition de serveur de connecteurs C++. La définition de serveur de connecteurs C++ peut se connecter au serveur de provisionnement directement, au lieu de passer par CA IAM CS. Cette solution a pour résultat la modification du groupe en une étape pour les comptes du connecteur CA Access Control. Toutefois, vous ne pouvez pas utiliser la console d'utilisateur pour gérer l'appartenance au groupe des comptes du connecteur CA Access Control. Pour cela, vous devez utiliser le gestionnaire de provisionnement.

Remarque : Pour plus d'informations sur l'utilisation de Connector Xpress pour créer une définition de serveur de connecteurs C++, reportez-vous à la rubrique How you Set a Managing Connector Server du manuel *Connector Xpress Guide*.

CA Arcot

Protection des tâches ArcotID lors de la protection de CA IdentityMinder par CA SiteMinder

Si CA SiteMinder protège CA IdentityMinder à l'aide d'un schéma d'authentification CA Arcot, les tâches suivantes ne fonctionnent pas dans CA IdentityMinder :

- Créer/Réinitialiser mon application ArcotID
- Télécharger mon application ArcotID

Les informations d'identification ArcotID activent l'authentification à deux facteurs pour les applications CA SiteMinder qu'un schéma d'authentification CA Arcot protège.

CA SiteMinder prend en charge uniquement un schéma d'authentification pour une ressource protégée. Toutes les tâches protégées CA IdentityMinder ont la même URL, qui est protégée par un schéma d'authentification CA SiteMinder.

N'utilisez pas l'authentification CA Arcot pour protéger l'URL pour accéder à des tâches protégées CA IdentityMinder.

Lorsque l'authentification CA Arcot protège l'URL des tâches protégées CA IdentityMinder, les utilisateurs doivent fournir un ID Arcot pour accéder aux tâches Créer/Réinitialiser mon application ArcotID ou Télécharger mon application ArcotID. Les utilisateurs qui accèdent à ces tâches n'ont pas encore d'ID Arcot et ne peuvent donc pas le fournir pour accéder aux tâches.

Pour empêcher ce problème lorsque CA SiteMinder protège des tâches CA IdentityMinder, utilisez un schéma d'authentification Active Directory ou LDAP, plutôt qu'un schéma d'authentification Arcot.

Remarque : Les tâches Créer/Réinitialiser mon application ArcotID ou Télécharger mon application ArcotID étant des tâches sensibles, il est fortement recommandé de les configurer comme des tâches protégées. Si vous les configurez comme des tâches publiques, les utilisateurs peuvent y accéder sans fournir d'informations d'identification.

Pour plus d'informations sur les tâches publiques, consultez la rubrique sur les tâches d'auto-administration du Manuel de conception de la console d'utilisateur.

Active Directory

Les sections suivantes décrivent les problèmes connus pour le connecteur d'Active Directory.

Résultats incorrects pendant la recherche dans la sous-arborescence avec le connecteur Active Directory

Lors de recherches dans des sous-arborescences contenant plusieurs unités organisationnelles et de nombreux objets dans chacune d'entre elles, il se peut que la recherche ne retourne aucun objet par erreur. Par exemple, dans une recherche limitée à 500, si le nombre d'objets de chaque unité organisationnelle dépasse cette limite, aucun résultat ne sera retourné. Même si le filtre de recherche réduit cette limite à moins de 500, il se peut que les résultats de cette recherche continuent d'être erronés et ne signalent aucun objet par erreur.

Solution

Augmentez la taille limite de la recherche.

Connecteur CA SSO pour serveur de stratégies avancé

Les sections suivantes décrivent les problèmes connus pour le connecteur CA SSO pour le serveur de stratégies avancé.

Limitation liée à l'ajout de comptes (2 000 maximum) dans les applications via le connecteur PLS

Vous ne pouvez pas ajouter plus de 2 000 comptes PLS à une application en même temps. Si vous devez ajouter plus de 2 000 comptes PLS, vous devrez diviser ces comptes en plusieurs opérations.

DB2 et DB2 de z/OS

Les sections suivantes décrivent les problèmes connus pour les connecteurs DB2 et DB2 z/OS.

Impossible d'enregistrer un type de données de date à cause d'une incohérence du type de données

Symptôme :

Lorsque je définis un attribut de type de date sur un terminal DB2 (JDBC DB2 pour IBM i), l'erreur suivante est affichée :

```
Bad SQL Grammar: Data type mismatch. (AAAA-MM-JJ)
```

Solution :

Modifiez l'URI de connexion de la page de terminal dans le gestionnaire de provisionnement et ajoutez *date format=iso*. L'URI s'affiche alors sous la forme : *jdbc:as400://<hôte>:CA Portal/<BdD>;prompt=false;date format=iso ;*. Tenez compte de l'espacement entre *date* et *format*.

E2Kx

Les sections suivantes décrivent les problèmes connus pour le connecteur E2Kx.

Erreur E2K CAFT lors de la gestion des droits des boîtes aux lettres

Lors de la gestion des droits des boîtes aux lettres, même si l'agent à distance Exchange est correctement configuré, il se peut qu'un message d'erreur CAFT indiquant un refus d'accès ou un échec lors de l'exécution de la commande apparaisse.

Cela peut se produire lorsque la liste des droits des boîtes aux lettres contient de multiples droits pour le même objet et que les objets Exchange gérés héritent des droits de l'objet parent.

Désynchronisation de la boîte aux lettres E2K7 après sa création

Lorsque vous sélectionnez l'option Utiliser la synchronisation forte pour créer un modèle de compte, puis que vous synchronisez un utilisateur global avec le modèle de compte, cliquez avec le bouton droit de la souris sur l'utilisateur global et sélectionnez Synchronisation des comptes. Les droits de la boîte aux lettres sont désynchronisés.

Solution

Sélectionnez Paramètres avancés Exchange, Droits de boîte aux lettres, Ajouter (Maj+méthode Ajouter), AUTORITE NT\Utilisateurs authentifiés, Lire les autorisations uniquement.

Adresses électroniques non définies dans les groupes de messagerie

Lorsque vous créez un groupe et que vous sélectionnez Créer une adresse de messagerie Exchange, aucune adresse électronique n'est définie pour le groupe.

Solution

Dans l'onglet Adresses électroniques, saisissez la nouvelle adresse électronique après création du groupe.

Affichage d'un message d'erreur lors de la tentative de modification d'un compte disposant d'une boîte aux lettres E27K

Lorsque vous tentez de modifier un compte disposant d'une boîte aux lettres E27K, un message d'erreur apparaît. Il s'agit d'une erreur sans importance : vous pouvez l'ignorer.

Message d'erreur de données manquantes lors de la tentative de création d'une boîte aux lettres E2Kx

Un message d'erreur indiquant que des caractères sont manquants apparaît dans le champ INT. Cette erreur ([-]?[\d]*) indique que le champ doit contenir des chiffres.

Impossible d'accepter simultanément des messages incluant ou excluant certains expéditeurs dans le gestionnaire de provisionnement en raison de limitations liées aux messages

Microsoft Exchange Server 2007 permet aux administrateurs de sélectionner les deux options suivantes : Accepter les messages provenant de/Uniquement les expéditeurs de la liste suivante et Rejeter les messages provenant de/Uniquement les expéditeurs de la liste suivante. Le gestionnaire de provisionnement permet de sélectionner uniquement une option. Microsoft Exchange 2003 présentait le même comportement. Si vous sélectionnez ces deux options en mode natif dans Microsoft Exchange 2007, cette fonctionnalité est décomposée dans le gestionnaire de provisionnement.

Google Apps

Les sections suivantes décrivent les problèmes connus pour le connecteur Google Apps.

Google Apps : message d'erreur lors de la création de comptes Google Apps

Symptôme :

Lorsque je crée un compte Google Apps, je reçois le message d'erreur suivant : *Echec de l'exécution de CreateGoogleAppsUser Le compte Google Apps a été créé, mais certaines opérations supplémentaires ont échoué*.

Le compte est créé dans CA IdentityMinder et sur le terminal Google Apps, mais il n'est pas visible dans la console d'utilisateur CA IdentityMinder parce qu'il n'est pas associé à l'utilisateur global.

Solution :

L'erreur se produit lorsque vous essayez de créer un compte à l'aide des mêmes surnom et nom d'utilisateur.

Pour résoudre le problème, lancez une exploration et une corrélation sur le terminal Google Apps.

Le compte créé est associé à l'utilisateur global dans CA IdentityMinder et est désormais visible.

Google Apps : terminaux Google Apps multiples sur la même instance de Java CS

Les paramètres de proxy du connecteur Google Apps sont des propriétés à l'échelle du système. Si vous créez deux terminaux Google Apps ou plus sur la même instance de Java CS, utilisez les mêmes serveur proxy, port, nom d'utilisateur et mot de passe.

Google Apps : message d'erreur "HTTP 403 : Refusé" reçu avec l'authentification NTLM

Symptôme :

Lorsque j'essaye d'utiliser l'authentification NTLM, je reçois l'erreur *HTTP 403 : Refusé* du serveur proxy et le domaine Google Apps n'est pas acquis.

Solution :

L'erreur se produit parce que sur un ordinateur Windows, Java CS est installé comme un service Windows et s'exécute comme un système local par défaut.

Si Java CS s'exécute sur un ordinateur Windows et si NTLM est le schéma d'authentification le plus fort pris en charge par le proxy HTTP, le connecteur Google Apps tente d'utiliser l'authentification NTLM avec le proxy HTTP.

Si votre serveur proxy HTTP utilise l'authentification NTLM, configurez Java CS afin qu'il s'exécute dans un compte de domaine Windows ou un compte local Windows.

Pour configurer l'authentification NTLM

Effectuez l'une des actions suivantes:

- Exécutez Java CS avec un compte Windows pouvant être authentifié avec le serveur proxy HTTP sans fournir un nom d'utilisateur et un mot de passe pour l'authentification du proxy lorsque vous créez le terminal.
- Exécutez Java CS avec un compte Windows ne pouvant pas être authentifié avec le serveur proxy HTTP, puis fournissez un nom d'utilisateur et un mot de passe HTTP pouvant être authentifiés avec le proxy lorsque vous créez le terminal.

Remarque : Si vous utilisez un utilisateur de domaine Windows pour l'authentification du proxy HTTP, préfixez le nom d'utilisateur de proxy HTTP avec le domaine Windows dans lequel l'utilisateur se trouve. Par exemple, DOMAINE\NomCompteUtilisateurProxy.

Echec d'une recherche de compte à partir de Google Apps

Symptôme :

Un échec de la recherche du prénom ou du nom associé à un compte Google Apps se produit.

Solution :

Les mises à jour apportées au prénom ou au nom d'un utilisateur peuvent prendre jusqu'à 30 minutes dans Google Apps. Par conséquent, un échec de la recherche du nouveau nom dans CA IdentityMinder peut se produire. Patientez 30 minutes après un changement de nom avant d'utiliser le nouveau nom dans la recherche.

PeopleSoft

Les sections suivantes décrivent les problèmes connus pour le connecteur PeopleSoft.

Les recherches peuvent échouer dans le gestionnaire de provisionnement

Lorsque vous utilisez le gestionnaire de provisionnement pour rechercher un terminal PeopleSoft avec PeopleTools 8.49, la recherche d'utilisateurs PPS pour l'affectation aux champs Autre ID d'utilisateur, Supervision de l'ID d'utilisateur et Réaffecter le travail à ne renvoie pas de résultats dans certains cas.

Il y a deux solutions pour ce problème :

- Utilisez la console d'utilisateur CA IdentityMinder pour gérer les terminaux PeopleSoft (solution préférée)
- Entrez la valeur dans les champs du gestionnaire de provisionnement sans effectuer de recherches. La valeur est encore soumise à validation, si bien que si la valeur entrée n'est pas un utilisateur PPS, l'affectation échoue lorsque vous cliquez sur le bouton Appliquer.

SAP

Les sections suivantes décrivent les problèmes connus pour le connecteur SAP.

Affectation de types d'utilisateurs contractuels SAP

Lorsque vous affectez un type d'utilisateur contractuel à un utilisateur dans l'onglet Données de la licence, le changement peut uniquement être appliqué au système principal et non au système enfant.

Solution

Vous pouvez modifier les types de licences contractuelles des enfants en mode natif.

Problème de préremplissage du terminal SAP à partir du fichier SAPlogon.ini

Si vous exécutez le gestionnaire de provisionnement sous Windows 2008, les détails du terminal pour SAP ne sont pas préremplis à partir du fichier SAPlogon.ini.

Remarque : Ce problème est propre aux exécutions du gestionnaire de provisionnement sous Windows 2008 uniquement.

Solution

Vous devez saisir manuellement le contenu du fichier SAPlogon.ini dans le gestionnaire de provisionnement.

Champs obligatoires dans l'attribut du type d'utilisateur contractuel SAP

Le type d'utilisateur contractuel spécifié dans l'onglet Données de licence du compte ne peut pas comporter de champs obligatoires autres que le champ LIC_TYPE. Par exemple, si vous devez spécifier le nom d'un système SAP R3 (SYSID) pour utiliser un type d'utilisateur contractuel, l'affectation échouera et une erreur indiquera qu'il manque une valeur pour le nom du système SAP R3.

Dysfonctionnement de l'attribut de type d'utilisateur contractuel pour certaines licences dans l'onglet Données de la licence du compte

Lorsque vous sélectionnez un type d'utilisateur dans la liste, seuls certains types d'utilisateurs fonctionnent. Certains types de licences renvoient une erreur d'appel de fonction BAPI. En fait, certains types d'utilisateurs contiennent des champs supplémentaires qui ne sont pas reconnus.

Siebel

Les sections suivantes décrivent les problèmes connus pour le connecteur Siebel.

Erreur SBL lors de la création d'un compte sur plusieurs terminaux

Un modèle de compte incluant plusieurs terminaux peut uniquement répertorier des groupes Siebel existants sur tous les terminaux.

Chapitre 5: Problèmes résolus

Ce chapitre traite des sujets suivants :

12.6.1

Les problèmes suivants ont été corrigés dans CA IdentityMinder 12.6.1 :

Ticket de support	Problème signalé
20576709/02	Prise en charge du partage du serveur de rapports BusinessObjects commun requise pour CA IdentityMinder et SiteMinder
20576725/02	Prise en charge du serveur de rapports BusinessObjects requise dans une configuration de haute disponibilité
20583665/02	Prise en charge du serveur de rapports BusinessObjects XI 3.1 SP5 (CABI 3.3) requise
20774861/02	Impossible d'inclure des données d'objet secondaires dans Policy Xpress
20777137/02	Améliorations apportées au flux de travaux basé sur une stratégie pour obtenir les objets secondaires (objets d'utilisateur) requis pour les objets principaux
20888199/01	Absence de documentation pour la convention d'attribution de nom unique pour les modèles de compte pour le service Web d'exécution des tâches
21073146/01	Synchronisation impossible avec la tâche Synchroniser les comptes avec le modèle de compte
21086870/01	Absence d'invite de saisie de clé FIPS dans le programme d'installation autonome de JCS, entraînant des problèmes de chiffrement
21108813/01	CA IdentityMinder 12.6 ne fournit pas les définitions de rôle attendues.
21111634/01	Création des journaux de terminal JCS impossible
21131768/01	Problème d'attribut de flux de travaux de la stratégie global (type d'objet secondaire manquants dans les définitions d'événement)
21135604/01	Echec de la tâche de gestionnaires d'attributs logiques avec une erreur NullPointer
21136454/01	Correction de la faille de sécurité liée à l'injection SQL dans cette version
21136456/01	Faille de sécurité
21136499/01	Les données des boîtes de sélection ne fonctionnent pas avec une fenêtre Profil associée à un service dans CA IdentityMinder 12.6.

Ticket de support	Problème signalé
21137701/01	Réception d'une exception PxEnvironmentException lors des appels de la stratégie Policy Xpress au code Java externe
21140501-1	Prise en charge des déploiements cloud (gestion de clients hébergés)
21146621/01	Validation globale des attributs dans directory.xml
21156269/01	Différences entre les schémas de base de données générés par le programme d'installation et les scripts de base de données dans le dossier d'outils
21156269/01	Plus de scripts requis pour la création manuelle de base de données
21162602/01	La corrélation personnalisée pour TSS ne fonctionne pas sur UNIX.
21170706/01	Les résultats de l'affichage des tâches soumises sont triés de manière incorrecte lorsque les paramètres régionaux sont définis sur Danois.
21175201/01	La synchronisation de compte initialisée par la notification entrante ne se produit pas lorsque les rôles de provisionnement sont affectés à l'aide de stratégies Policy Xpress.
21181592/01	Echec du chargement de CA IdentityMinder r12.6 avec une erreur de chemin d'accès de classe non valide
21183366/01	Nom d'utilisateur incorrect utilisé avec les sources de données
21187385/01	Arrêts intermittents de CA IdentityMinder
21188814/01	Le serveur de stratégies de SiteMinder r12 SP3 CR11 tombe en panne lors de l'accès à la stratégie CA IdentityMinder.
21190699/01	Impossible de récupérer les informations d'objet secondaires à partir de Policy Xpress sur les stratégies basées sur les événements ou sur les tâches. Les informations de valeur d'attribut d'origine sont également renvoyées, même lorsque Policy Xpress se déclenche après la fin de la tâche.
21190873/01	508 Problème de conformité : les info-bulles des cases à cocher sont incompréhensibles.
21193837/01	Création et suppression d'objets gérés
21194712-1	Policy Xpress avec itérateur s'interrompt lorsqu'une affectation de rôle d'accès déclenchée est rejetée par le flux de travaux.
21200396/01	508 Problème de conformité : problèmes avec le lien Passer directement au contenu principal
21200412/01	508 Problème de conformité : les messages d'erreur et d'avertissement ne sont pas lus correctement par le logiciel d'assistance aux utilisateurs handicapés.
21213029-1	Les variables de services de mot de passe stockées dans le cache de JSession ne sont pas effacées lors de la déconnexion et les demandes ultérieures sont redirigées vers la page pws.fcc.

Chapitre 6: Documentation

Les noms de fichier des manuels de CA IdentityMinder sont les suivants :

Nom du manuel	Nom du fichier
Notes de parution	im_release_fra.pdf
Manuel d'implémentation	im_impl_enu.pdf
Installation Guide for WebLogic (Manuel d'installation pour WebLogic)	im_install_weblogic_enu.pdf
Installation Guide for WebSphere (Manuel d'installation pour WebLogic)	im_install_websphere_enu.pdf
Installation Guide for JBoss (Manuel d'installation pour WebLogic)	im_install_jboss_enu.pdf
Upgrade Guide (Manuel de mise à niveau)	im_upgrade_enu.pdf
Configuration Guide (Manuel de configuration)	im_config_enu.pdf
Administration Guide (Manuel d'administration)	im_admin_enu.pdf
User Console Design Guide (Manuel de conception de la console d'utilisateur)	im_uc_design_enu.pdf
Programming Guide for Java (Manuel de programmation pour Java)	im_dev_enu.pdf
Provisioning Reference Guide (Manuel de référence du provisionnement)	im_provisioning_reference_enu.pdf
Connectors Guide (Manuel des connecteurs)	im_connectors_enu.pdf
Connector Xpress Guide (Manuel des connecteurs Xpress)	im_connector_xpress_enu.pdf
Java Connector Server Implementation Guide (Manuel d'implémentation du serveur de connecteurs Java)	im_jcs_impl_enu.pdf
Programming Guide for Java Connector Server (Manuel de programmation du serveur de connecteurs Java)	im_jcsProg_Enu.pdf
Glossaire	im_glossary.pdf
Bibliothèque	im_bookshelf_enu.zip

Ce chapitre traite des sujets suivants :

Bibliothèque

La bibliothèque permet d'accéder à l'ensemble de la documentation CA IdentityMinder à partir d'une interface unique. Elle contient :

- Une liste extensible du contenu de tous les manuels au format HTML
- Une fonctionnalité de recherche de texte intégral dans l'ensemble des manuels, avec classement des résultats des recherches et termes recherchés mis en surbrillance dans le contenu
- Des chemins de navigation reliés aux rubriques du niveau supérieur
- Un index HTML unique des rubriques pour tous les manuels
- Des liens vers les versions PDF des manuels pour impression

Pour utiliser la bibliothèque :

1. Téléchargez la bibliothèque sur le site de support de CA.
2. Extrayez le contenu du fichier ZIP.

   Remarque : Pour de meilleures performances lors de l'installation de la bibliothèque sur un système distant, accédez à cette bibliothèque à partir d'un serveur Web.
3. Affichez la bibliothèque comme indiqué ci-après.
   - Si la bibliothèque se trouve sur un système local et que vous utilisez Internet Explorer, ouvrez le fichier Bookshelf.hta.
   - Si la bibliothèque se trouve sur un système distant ou que vous utilisez Mozilla Firefox, ouvrez le fichier Bookshelf.html.

     Remarque : Pour de meilleures performances lors de l'installation de la bibliothèque sur un système distant, accédez à cette bibliothèque à partir d'un serveur Web.

La bibliothèque nécessite Internet Explorer 7 ou 8, ou Mozilla Firefox 2 ou 3. Pour les liens vers les manuels au format PDF, Adobe Reader 7 ou version supérieure est nécessaire. Vous pouvez télécharger Adobe Reader à l'adresse www.adobe.com.

Notes de parution relatives à l'intégration de CA IdentityMinder et CA RCM

Toutes les notes de parution relatives à l'intégration de CA IdentityMinder et CA RCM se trouvent dans les *Notes de parution de CA RCM*. Vous pouvez accéder à la bibliothèque de CA RCM à partir du site de support de CA.

Annexe A: Fonctionnalités d'accessibilité

CA Technologies s'engage à ce que tous ses clients puissent, quelles que soient leurs capacités, utiliser sans problème ses produits et les documentations associées pour réaliser des tâches commerciales cruciales. Cette section présente les fonctions d'accessibilité intégrées de CA IdentityMinder.

508 Conformité

CA IdentityMinder est conforme à la Section 508 de la norme US Rehabilitation Act et au niveau AA des directives Web Content Accessibility Guidelines (WCAG2.0). Pour plus d'informations, reportez-vous à la rubrique Améliorations apportées au produit (page 71). Vous pouvez également demander à votre responsable de compte une copie du document Voluntary Product Accessibility Template (VPAT) de CA Technologies.

Améliorations du produit

Des améliorations relatives à l'accessibilité ont été apportées dans les zones suivantes de *CA IdentityMinder* :

- Affichage
- Son
- Clavier
- Souris

Remarque : Les informations suivantes s'appliquent aux applications basées sur Windows et sur Macintosh. Les applications Java s'exécutent sur différents systèmes d'exploitation hôtes, qui disposent déjà de technologies d'assistance. Pour que les technologies d'assistance existantes puissent accéder aux programmes écrits en JPL, un pont est nécessaire entre ces technologies dans leurs environnements natifs et la prise en charge de Java Accessibility qui est disponible à partir de la machine virtuelle Java. Ce pont connecte la machine virtuelle Java et la plate-forme native, et sera donc légèrement différent selon la plate-forme utilisée. Sun développe actuellement les parties JPL et Win32 de ce pont.

Affichage

Pour augmenter la visibilité sur l'écran de votre ordinateur, vous pouvez ajuster les options suivantes :

Style de police, couleur et taille des éléments

Permet de choisir la couleur de la police, la taille et d'autres combinaisons visuelles.

Résolution d'écran

Permet de modifier le nombre de pixels pour agrandir des objets dans la fenêtre.

Largeur du curseur et fréquence de clignotement

Permet de rendre le curseur plus facile à trouver ou de réduire le clignotement.

Taille de l'icône

Permet d'agrandir les icônes pour augmenter la visibilité ou de réduire l'espace de la fenêtre.

Schémas de contraste élevé

Permet de sélectionner des combinaisons de couleur qui sont plus faciles à voir.

Son

Utilisez le son en cas de déficience visuelle ou pour faciliter l'écoute des sons émis par l'ordinateur en ajustant les options suivantes :

Volume

Permet de monter ou de baisser le son de l'ordinateur.

Conversion de texte par synthèse vocale

Permet d'écouter les options de commande et de lire le texte par synthèse vocale.

Avertissements

Permet d'afficher des avertissements visuels.

Avertissements

Permet d'émettre des avertissements visuels ou oraux selon que les fonctionnalités d'accessibilité sont activées ou désactivées.

Schémas

Permet d'associer les sons de l'ordinateur à des événements système spécifiques.

Légendes

Permet d'afficher des légendes pour la fonction vocale et les sons.

Remarque : Si vous utilisez un lecteur d'écran, il est recommandé d'installer la dernière version de l'outil pour une interprétation optimale.

Clavier

Vous pouvez effectuer les réglages de clavier suivants :

Vitesse de répétition

Permet de définir la vitesse de répétition d'un caractère lorsque vous appuyez sur une touche.

Tonalités

Permet d'émettre des tonalités lorsque vous appuyez sur certaines touches.

Touches collées

Permet à ceux qui utilisent le clavier avec une main ou un doigt de choisir des dispositions de clavier plus adaptées.

Lien Ignorer

Vous permet d'utiliser le lien Ignorer et revenir au contenu principal pour accéder rapidement au contenu principal.

Souris

Vous pouvez utiliser les options suivantes afin de rendre votre souris plus rapide et plus facile à utiliser :

Vitesse de clic

Permet de définir la vitesse de clic de la souris lorsque vous effectuez une sélection.

Verrouillage de clic

Permet une mise en surbrillance ou un glissement sans devoir maintenir le bouton de la souris enfoncé.

Inverser

Vous permet d'inverser les fonctions contrôlées par les touches de gauche et de droite de la souris.

Fréquence de clignotement

Vous permet d'activer le clignotement du curseur et de choisir sa vitesse.

Options du pointeur

Vous permet d'effectuer les opérations suivantes :

- Masquer le pointeur lors de la saisie
- Afficher l'emplacement du pointeur
- Définir la vitesse de déplacement du pointeur déplace dans la fenêtre
- Sélectionner la taille et la couleur du pointeur pour une meilleure visibilité
- Déplacer le pointeur vers un emplacement par défaut dans une boîte de dialogue

Exceptions Mozilla FireFox

Il est recommandé que les utilisateurs de clavier et de JAWS utilisent Internet Explorer 8, pour les raisons suivantes :

- Dans Firefox, les boîtes de dialogue ne reçoivent pas le focus d'entrée/de sortie.
- Le lien Ignorer et revenir au contenu principal n'est pas toujours lu d'abord par le lecteur d'écran.

Raccourcis clavier

La table suivante répertorie les raccourcis clavier pris en charge dans CA IdentityMinder :

Clavier	Description
Ctrl+X	Couper
Ctrl+C	Copier
Ctrl+K	Rechercher le suivant
Ctrl+F	Rechercher ou remplacer
Ctrl+V	Coller
Ctrl+S	Enregistrer
Ctrl+Maj+S	Tout enregistrer
Ctrl+D	Supprimer la ligne
Ctrl+flèche droite	Mot suivant
Ctrl+flèche vers le bas	Défilement de la ligne vers le bas
End	Fin de ligne